TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL
NEW DELHI

Dated 24th September, 2019

Cyber Appeal No.5 of 2013

ICICI Bank Ltd. ... Appellant
Versus
Mr.Saurabh Ravi Shankar Jain and Another ... Respondents

BEFORE:

HON'BLE MR. JUSTICE SHIVA KIRTI SINGH, CHAIRPERSON
HON'BLE MR. A.K. BHARGAVA, MEMBER

For Appellant : Mr.Hemant Gupta, Advocate
Mr.Alok Sharma, Advocate

For Respondent No.2 : Ms.Akanksha Banerjee,Advocate
Ms.Sonakshi Banerjee, Advocate

ORDER

Heard learned counsel for the appellant and learned counsel for Respondent No.2, Vodafone Idea Ltd. The Respondent No.1/complainant was served with notice but has chosen not to appear and, therefore, the appeal has been heard *ex parte qua* Respondent No.1.

2. This appeal is filed under sections 57 and 58 (2) of the Information Technology Act,2000 (hereinafter referred to as "the Act"). Appellant is aggrieved by the impugned order dated 22.2.2013 passed by the Adjudicating Officer (A.O.), the then Secretary (Information Technology), Government of Maharashtra. The

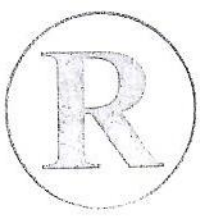
operative part of the impugned order discloses that the A.O. has found the appellant very lax and negligent and thereby it had failed to prevent the offence under sections 43 and 43A of the Act and, therefore, out of the total loss incurred by the complainant of Rs.2.02 lakh, the appellant has been directed to pay damages to the tune of Rs.1.5 lakh by way of compensation to the complainant.

3. The A.O. has also found respondent no. 2 deficient in not following the reasonable security practices and procedures before issuing a duplicate SIM card which caused wrongful loss to the complainant. He held respondent no. 2 also to be in violation of section 43 of the Act and has ordered it to pay damages to the tune of Rs. 25,000/- by way of compensation to the complainant. The remaining loss of Rs. 27,000/- has been left to be borne by the complainant.

4. Learned counsel for the appellant has taken us through the facts of the case which shows that the complainant's saving account with a branch of the appellant bank in Pune suffered a fraudulent withdrawal of Rs. 2.02 Lakh on 15.10.2010 and 16.10.2010 through 15 fraudulent transactions. The money was transferred into three other accounts of ICICI Bank from where it was withdrawn by the fraudsters. According to Police investigation, the account holders were fictitious and not traceable.

5. The defence is twofold: firstly, it has been urged that the complainant was negligent, deserving no compensation because the transfer could not have been possible without his having compromised the password and his ID to the fraudster. Secondly, it has been highlighted that bank had in place a good security system of sending OTPs for such transactions involving transfer of money to any beneficiary and that security system was compromised apparently because of wrong issuance of duplicate SIM card by respondent no. 2. The plea is that if duplicate SIM card had not been issued and the original SIM had not been deactivated, the OTPs would have reached the complainant and the fraud could have been prevented.

6. In support of the first plea that the complainant was negligent and responsible for the fraud, it has been urged that the complainant in his communications and complaints to various authorities admitted that he had responded to a phishing mail divulging his ID and password. The order of the A.O. discloses that such defence was urged on behalf of the appellant and even after presuming such a defence to be plausible, the A.O. found the appellant lacking in proper security. However, while recording his conclusions in paragraph 13(a), the A.O. has made it clear that complainant responding to a phishing mail is only a presumption and there is no proof for the same.



7. In view of the above conclusions by the A.O., we gave opportunity to learned counsel for the appellant to show any evidence including complaints or communications from the complainant in support of the defence noted above but no material by way of evidence was brought to our notice. The appellant has failed to bring on record any communication from the complainant which could show that he had admitted to have received a phishing mail leading to disclosure of his ID and password.

8. While on this issue it is submitted on behalf of the appellant that a fraudster cannot succeed in transferring money from the account holder of the bank unless it is able to find out a customer's user ID and password. A bank account holder may become a victim of fraud through various methods leading to compromise of his ID and password. It may happen even if the account holder is not negligent to any appreciable degree. Sometimes materials originating from bank's IP/domain name may have assurance of creditability and can deceive many customers. Adequate security requires protecting the account holders from loss by creating further layers of security so as to prevent frauds even if for some reason user ID and password has been compromised and also to protect the account holder from repetition of the fraud on the same day or on the next day. OTPs, Balance statements, warnings or even freezing the account may be methods of security to protect the customers. In the present case, in the pleadings some general defence has been taken about

adequacy of security measures adopted by the bank but there is absolute lack of specific and definite pleadings that any of the measures were applied and used in the present case of the complainant/victim. There is no averment that any OTP or any other kind of communication regarding fraudulent withdrawals was sent by the bank to the victim at any given date or time. Not only pleadings are deficient and virtually absent, there is also no evidence led by the bank documentary or otherwise to show that any security measures were applied in the case of the complainant.

9. In view of nature of the pleadings and the lack of proof, we are not persuaded to accept that the appellant bank had established good and healthy security measures and those were operational and were used for avoiding fraud in the case of the complainant. Sections 43 and 43A of the Act create such responsibility on the bank because it stores sensitive data of its account holders in its computer system. In our considered view, appellant bank has failed to show that at the relevant time it had put in place adequate and reasonable security measures.

10. The other plea urged on behalf of the appellant is with a view to hold respondent no. 2 liable for a further amount of money for a contributory negligence. Before coming to this issue, it will be useful to note that since the amount awarded against respondent no. 2 was only 25,000/-, it chose to pay that

amount to the complainant instead of filing any appeal. This stand was taken when respondent no. 2 appeared in this appeal and that explains why no cross appeal has also been filed once the amount was accepted and paid. In view of such factual situation, a categorical stand has been taken on behalf of respondent no. 2 that the legal issue as to whether a telecom service provider like the respondent no. 2, can be made liable under the IT Act for the lapse of issuing a duplicate SIM to a wrong person, should be left upon to be decided in appropriate case where the telecom company has preferred appeal or cross appeal. We accept the aforesaid submission and leave those issues of law open for determination in an appropriate case. Hence, for the present case it is presumed that the findings of the A.O. against respondent no. 2 are correct. But on facts it remains to be examined whether respondent no. 2 can be held to be equally or more negligent than the appellant so as to be made liable for paying a higher compensation.

11. In reply to such a stand of the appellant, learned counsel for the respondent no 2 has taken us through the impugned order of the A.O., particularly to paragraphs 4,5 and 6. In those paragraphs the A.O. has held the appellant responsible for negligent on many counts. The A.O. has highlighted the role of the bank by noting that for even sending a phishing mail, the fraudster has to know a few details about the victim which are available with the bank including his email ID and mobile number. He has also noted that the bank did not have a healthy

security system in place because it could not even trace the IP address from where the fraudulent transactions took place. The A.O. has also noted that apparently the beneficiary accounts which were also with the ICICI BANK, had been opened without proper compliance with KYC norms because as per police report those account holders were fictitious person. Learned counsel for the respondent no. 2 has submitted that in its reply respondent no. 2 has taken the defence that it has duly followed the complete procedure of issuing duplicate SIM cards which was done on an application made for the purpose. The proof of identity document used was forged copy of a driving licence, which was submitted along with a forged FIR but the respondent no. 2 had no capability or means for detecting the said forgery. According to her, in any case, respondent no. 2 cannot be presumed to be involved in forgery in view of a judgement of this Tribunal dated 12.04.2012 in Petition No. 252 of 2011 (COAI & Ors. Vs. Department of Telecommunications & Anr). She has relied upon paragraph-193 of the judgement enclosed as Annexure 'A' to the reply filed on 01.07.2019. The aforesaid judgement in the case of COAI made the relevant observations in paragraph-193 while considering a matter in the background of scrutiny of subscriber's application at the time of issuance of SIM for the first time and the prescribed KYC norms provided for the same. In our considered view, the situation will be different at the time of issuance of duplicate SIM when the subscriber is already known to the telecom operator who has his relevant data in its system. However, for the negligence of respondent no. 2 the

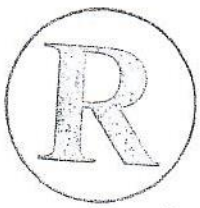
A.O has saddled it with liability to pay Rs. 25,000/-. This is clearly on account of respondent no. 2, being held responsible for contributory negligence.

12. The next plea of the appellant that for the contributory negligence found against it, respondent no. 2 should be saddled with higher damages, has not been supported by any good reasons particularly when learned counsel for the respondent no. 2, has shown from various paragraphs of the judgement under appeal, that the appellant has been found deficient in its security system on various grounds. Since we are in agreement with the finding that appellant's security system was deficient, in the facts of the case, we are not persuaded to interfere with the findings of the A.O. and his awarding different compensation amounts payable by the appellant and respondent no. 2. On the issue of apportionment of damages in a case of contributory negligence, there is neither enough pleadings nor any case law has been brought to our notice. Hence, we leave that issue also open for consideration in any appropriate case.

13. In view of the aforesaid discussions and findings, we find no good reason to interfere with the impugned order. The appeal is accordingly dismissed. There shall be no order as to costs.

14. We direct that a copy of this judgment be sent to the concerned A.O. who shall ensure that the amount payable by the appellant, if not paid already to the

complainant, is paid and the order of the A.O. is executed at an early date, preferably within two months of receipt of a copy of the judgement. The appellant is also directed to pay to the complainant the comprehension amount in terms of impugned order of the A.O. within two months from today, if the amount has not been paid already.



(S. K. Singh, J)
Chairperson

(A.K. Bhargava)
Member

dbc